UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/506,830	02/18/2000	Daniel I Flitcroft	032668-006	9055

21839 7590 12/31/2002

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
GRAHAM, CLEMENT B

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 12/31/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/506,830	FLITCROFT ET AL.	
	Examiner	Art Unit	
	Clement B Graham	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *amendment filed 9 October 2002* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-21 are remained and 22-28 has been added.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-5, 11-19, 20-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al U.S. Patent No. 5883810.

As per claims 1, 3, Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy

for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer).

The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin et al). Franklin does not explicitly teach limited use credit card number that is not yet activated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to that the teachings of Franklin et al can be applied to accomplish the teachings of the claimed invention and in order for a credit card that was been issued to be activated. The benefit would have been to validate the credit card number by an issuing authority upon a customer attempting to perform a transaction using the credit card number.

As per claim 2, Franklin et al discloses for added security, the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction. For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID. The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 50-55 of Franklin et al). Franklin et al does explicitly teach specific group of merchants. It would have been obvious to one of ordinary skill in the art at the time the invention was made to that the teachings of Franklin et al can be applied in order use a specific group of merchants, in order to achieve the claimed invention. The benefit would have been to have a credit card number with limitations set within the card by the issuing authority.

As per claim 4, Franklin et al discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations. (See column 7 lines 5-30 of Franklin et al). Franklin et al also discloses for added security, the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction. For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID. The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 50-55 of Franklin et al). Franklin et al does not explicitly teach requesting validation of a limited use credit card for a merchant as identified by a merchant identification number. It would have been obvious to one of ordinary skill in the art at the time the invention was made to that the teachings of Franklin et al can be applied in order to validate a limited use credit card for a merchant as identified by a merchant identification number. The benefit would

have been to validate a credit card number and execute the limited use function of the card.

As per claim 5, Franklin et al discloses during the payment authorization phase, the merchant submits the transaction number over the conventional payment network to the issuing bank for approval. The issuing bank identifies the number as a transaction number, as opposed to a real customer account number. The issuing bank uses the transaction number to retrieve the data record linking the transaction number to a customer account number. The issuing bank then swaps the customer account number for the transaction number and processes the authorization request using its conventional processing system. After the processing, the issuing bank substitutes the transaction number back for the customer account number and returns the authorization reply to the merchant under the transaction number. In this manner, only the issuing bank is aware that the transaction number is a proxy for the customer account number. The merchant need not be aware that the transaction number is not a true customer account number, but simply handles the number as it would any other card number. (See column 5 of Franklin et al). Franklin also discloses the issuing institution can use the existing processing system to check account information spending limits, and so forth.(See column 2 lines 30-40 of Franklin et al). Franklin also discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 line 50 of Franklin et al). Franklin does not explicitly teach deactivating the limited use credit card number by the card issuer when a triggered condition is present. It would have been obvious to one of ordinary skill in the art at the time the invention was made that

the teachings of Franklin et al can be applied in order to deactivate the limited use credit card number by the card issuer when a triggered condition is present. The benefit would have been to tender the credit card number to a merchant to pay for merchandise further deactivating the limited use credit card when the transaction is completed.

As per claims 11-12, Franklin discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 30-50 of Franklin et al). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin et al in order to for a short expiration term or spending limits placed on the transaction number which will trigger an invalid card. The benefit would have been to enforce a restriction associated with the transaction number.

As per claim 15, It would have obvious to one of ordinary skill in the art at the time the invention was made that declining authorization for credit card transaction is a common function in the art. The benefit would have been to authenticate a transaction before it is given approval.

As per claim 13-14, Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a

single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al does not explicitly teach limited use properties of revalidated limited use credit card number are different from the limited use properties of the validated limited use credit card number this is taught by Masuda. Masuda discloses the credit card and/or the first system may have a limit amount column for recording a limit amount of money, and the first system may further comprise

means for updating the limit amount of money recorded in the limit amount column as the credit card is used. Each of the methods may further comprise the step of determining whether the credit card can be used or not based on resultant data produced by comparison between the limit amount of money recorded in the limit amount column and an amount to money proposed to pay with the credit card. It would have been obvious to one of ordinary skill in the art at the time that invention was made to modify the teachings of Franklin et al to include Masuda in order for the limited use properties of revalidated limited use credit card number to be different from the limited use properties of the validated limited use credit card number. The benefit would have been to reactivate or update the credit card with a new value.

As per claims 16, Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular

credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth.

Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module 56 and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard 56 generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such

tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin et al). Franklin does not explicitly teach limited use credit card number that is not yet activated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to note that the teachings of Franklin et al can be applied to accomplish the teachings of the claimed invention and in order for a credit card that was been issued to be activated. The benefit would have been to validate the credit card number by an issuing authority upon a customer attempting to perform a transaction using the credit card number.

As per claim 17, Franklin discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 30-50 of Franklin et al). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin et al in order to for a short expiration term or spending limits placed on the transaction number which will trigger an invalid card. The benefit would have been to enforce a restriction associated with the transaction number.

As per claims 18, 20-21, Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a

transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a

"request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin et al). Franklin does not explicitly teach limited use credit card number that is not yet activated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to note that the teachings of Franklin et al can be applied to accomplish the teachings of the claimed invention and in order for a credit card that was been issued to be activated. The benefit would have been to validate the credit card number by an issuing authority upon a customer attempting to perform a transaction using the credit card number.

As per claim 19, Franklin discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 30-50 of Franklin et al). It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the teachings of Franklin et al in order to for a short expiration term or spending limits placed on the transaction number which will trigger an invalid card. The benefit would have been to enforce a restriction associated with the transaction number.

As per claims 22-28, Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party

certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth.

Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See

column 2 lines 5-40 of Franklin et al). Franklin et al also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module 56 and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard 56 generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin et al). Franklin does not explicitly teach limited use credit card number that is not yet activated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to note that the teachings of Franklin et al can be applied to accomplish the teachings of the claimed invention and in order for a credit card that was been issued to be activated. The benefit would have been to validate the credit card number by an issuing authority upon a customer attempting to perform a transaction using the credit card number.

3. Claims 6-7, 8-10, are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al U.S. Patent No. 5883810 in view of Hidehiro Masuda U.S. Patent No 5,777,306.

As per claim 6-7, Franklin discloses the issuing institution can use the existing processing system to check account information spending limits, and so forth.(See

column 2 lines 30-40 of Franklin et al). Franklin also discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 line 50 of Franklin et al). Franklin does not explicitly teach communicating with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating step or revalidating the use credit card number with associated limited use properties this is taught by Masuda. Masuda discloses the credit card and/or the first system may have a limit amount column for recording a limit amount of money, and the first system may further comprise means for updating the limit amount of money recorded in the limit amount column as the credit card is used. Each of the methods may further comprise the step of determining whether the credit card can be used or not based on resultant data produced by comparison between the limit amount of money recorded in the limit amount column and an amount to money proposed to pay with the credit card. It would have been obvious to one of ordinary skill in the art at the time that invention was made to modify the teachings of Franklin et al to include Masuda in order to communicate with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating. The benefit would have been to reactivate or update the credit card with a new value.

As per claim 8-10, Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer

account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al does explicitly not teach limited use

properties of revalidated limited use credit card number are different from the limited use properties of the validated limited use credit card number this is taught by Masuda. Masuda disclose the credit card and/or the first system may have a limit amount column for recording a limit amount of money, and the first system may further comprise means for updating the limit amount of money recorded in the limit amount column as the credit card is used. Each of the methods may further comprise the step of determining whether the credit card can be used or not based on resultant data produced by comparison between the limit amount of money recorded in the limit amount column and an amount to money proposed to pay with the credit card. It would have been obvious to one of ordinary skill in the art at the time that invention was made to modify the teachings of Franklin et al to include Masuda in order for the limited use properties of revalidated limited use credit card number to be different from the limited use properties of the validated limited use credit card number. The benefit would have been to reactivate or update the credit card with a new value.

Response to Arguments

5. Applicant's arguments files on 10/09/02 have been fully considered but they are not persuasive for the following reasons.

6. In response to applicant's arguments regarding Franklin and Masuda.

In response to applicant's arguments regarding **1, 3,** Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to

remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal

carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin et al). Franklin does not explicitly teach limited use credit card number that is not yet activated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to that the teachings of Franklin et al can be applied to accomplish the teachings of the claimed invention and in order for a credit card that was been issued to be activated. The benefit would have been to validate the credit card number by an issuing authority upon a customer attempting to perform a transaction using the credit card number.

In response to applicant's arguments regarding **claim 2**, Franklin et al discloses for added security, the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction. For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID. The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 50-55 of Franklin et al). Franklin et al does explicitly

teach specific group of merchants. It would have been obvious to one of ordinary skill in the art at the time the invention was made to that the teachings of Franklin et al can be applied in order use a specific group of merchants, in order to achieve the claimed invention. The benefit would have been to have a credit card number with limitations set within the card by the issuing authority.

In response to applicant's arguments regarding **As per claim 4**, Franklin et al discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations. (See column 7 lines 5-30 of Franklin et al). Franklin et al also discloses for added security, the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction. For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID. The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration

term lapses. (See column 2 lines 50-55 of Franklin et al). Franklin et al does not explicitly teach requesting validation of a limited use credit card for a merchant as identified by a merchant identification number. It would have been obvious to one of ordinary skill in the art at the time the invention was made to that the teachings of Franklin et al can be applied in order to validate a limited use credit card for a merchant as identified by a merchant identification number. The benefit would have been to validate a credit card number and execute the limited use function of the card.

In response to applicant's arguments regarding **claim 5**, Franklin et al discloses during the payment authorization phase, the merchant submits the transaction number over the conventional payment network to the issuing bank for approval. The issuing bank identifies the number as a transaction number, as opposed to a real customer account number. The issuing bank uses the transaction number to retrieve the data record linking the transaction number to a customer account number. The issuing bank then swaps the customer account number for the transaction number and processes the authorization request using its conventional processing system. After the processing, the issuing bank substitutes the transaction number back for the customer account number and returns the authorization reply to the merchant under the transaction number. In this manner, only the issuing bank is aware that the transaction number is a proxy for the customer account number. The merchant need not be aware that the transaction number is not a true customer account number, but simply handles the number as it would any other card number. (See column 5 of Franklin et al). Franklin also discloses the issuing institution can use the existing processing system to check account information spending limits, and so forth.(See column 2 lines 30-40 of Franklin

et al). Franklin also discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 line 50 of Franklin et al). Franklin does not explicitly teach deactivating the limited use credit card number by the card issuer when a triggered condition is present. It would have been obvious to one of ordinary skill in the art at the time the invention was made that the teachings of Franklin et al can be applied in order to deactivate the limited use credit card number by the card issuer when a triggered condition is present. The benefit would have been to tender the credit card number to a merchant to pay for merchandise further deactivating the limited use credit card when the transaction is completed.

In response to claims **11-12**, Franklin discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 30-50 of Franklin et al). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin et al in order to for a short expiration term or spending limits placed on the transaction number which will trigger an invalid card. The benefit would have been to enforce a restriction associated with the transaction number.

In response to **claim 15**, It would have obvious to one of ordinary skill in the art at the time the invention was made that declining authorization for credit card transaction is a common function in the art. The benefit would have been to authenticate a transaction before it is given approval.

In response to **claim 13-14**, Franklin et al discloses an online commerce card is issued

electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an

authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al does not explicitly teach limited use properties of revalidated limited use credit card number are different from the limited use properties of the validated limited use credit card number this is taught by Masuda. Masuda discloses the credit card and/or the first system may have a limit amount column for recording a limit amount of money, and the first system may further comprise means for updating the limit amount of money recorded in the limit amount column as the credit card is used. Each of the methods may further comprise the step of determining whether the credit card can be used or not based on resultant data produced by comparison between the limit amount of money recorded in the limit amount column and an amount to money proposed to pay with the credit card. It would have been obvious to one of ordinary skill in the art at the time that invention was made to modify the teachings of Franklin et al to include Masuda in order for the limited use properties of revalidated limited use credit card number to be different from the limited use properties of the validated limited use credit card number. The benefit would have been to reactivate or update the credit card with a new value.

In response to **claims 16,** Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the

customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon

receiving the PIN, the customer invokes the registration module 56 and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard 56 generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin et al). Franklin does not explicitly teach limited use credit card number that is not yet activated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to note that the teachings of Franklin et al can be applied to accomplish the teachings of the claimed invention and in order for a credit card that was been issued to be activated. The benefit would have been to validate the credit card number by an issuing authority upon a customer attempting to perform a transaction using the credit card number.

In response to **claim 17**, Franklin discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 30-50 of Franklin et al). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin et al in order to for a short expiration term or spending limits placed on the transaction number which will trigger an invalid card. The benefit would have been to enforce a restriction associated with the transaction number.

In response to claims **18, 20-21,** Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth.

Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin et al also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin et al). Franklin does not explicitly teach limited use credit card number that is not yet activated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to note that the teachings of Franklin et al can be applied to accomplish the teachings of the claimed invention and in order for a credit card that was been issued to be activated. The benefit would have been to validate the credit card number by an issuing authority upon a customer attempting to perform a transaction using the credit card number.

In response to **claim 19**, Franklin discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid

after the expiration term lapses. (See column 2 lines 30-50 of Franklin et al). It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the teachings of Franklin et al in order to for a short expiration term or spending limits placed on the transaction number which will trigger an invalid card. The benefit would have been to enforce a restriction associated with the transaction number.

In response to **claim 6-7**, Franklin discloses the issuing institution can use the existing processing system to check account information spending limits, and so forth.(See column 2 lines 30-40 of Franklin et al). Franklin also discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 line 50 of Franklin et al). Franklin does not explicitly teach communicating with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating step or revalidating the use credit card number with associated limited use properties this is taught by Masuda. Masuda discloses the credit card and/or the first system may have a limit amount column for recording a limit amount of money, and the first system may further comprise means for updating the limit amount of money recorded in the limit amount column as the credit card is used. Each of the methods may further comprise the step of determining whether the credit card can be used or not based on resultant data produced by comparison between the limit amount of money recorded in the limit amount column and an amount to money proposed to pay with the credit card. It would have been obvious to one of ordinary skill in the art at the time that invention was made to modify

the teachings of Franklin et al to include Masuda in order to communicate with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating. The benefit would have been to reactivate or update the credit card with a new value.

In response to **claim 8-10**, Franklin et al discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate

data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin et al). Franklin et al does explicitly not teach limited use properties of revalidated limited use credit card number are different from the limited use properties of the validated limited use credit card number this is taught by Masuda. Masuda disclose the credit card and/or the first system may have a limit amount column for recording a limit amount of money, and the first system may further comprise means for updating the limit amount of money recorded in the limit amount column as the credit card is used. Each of the methods may further comprise the step of determining whether the credit card can be used or not based on resultant data produced by comparison between the limit amount of money recorded in the limit amount column and an amount to money proposed to pay with the credit card. It would have been obvious to one of ordinary skill in the art at the time that invention was made to modify the teachings of Franklin et al to include Masuda in order for the limited use properties of revalidated limited use credit card number to be different from the limited use properties of the validated limited use credit card number. The benefit would have been to reactivate or update the credit card with a new value.

8. **Note is taken** by the examiner that should the applicant find objectionable any

statements made herein by the examiner regarding inherency, implicitness, obviousness, or Official Notice, Applicant can make a proper challenge to those statements only by providing adequate information or argument so that on its face it creates a reasonable doubt regarding the circumstances justifying those statements: a simple response requesting a reference without doing so, or a response that fails to logically refute the basic assumptions underlying the justification, will result in an improper and failed challenge and those unchallenged statements will remain the record of the case. Applicants must seasonably challenge those statements in the first response following an Office Action. If an applicant fails to do so, his right to challenge them is waived.

9. In response to applicant arguments against the references individually, one cannot show nonobviousness by attacking the reference individually where the rejections are based on a combination of references. See In Keller, 642 F.2d, 208 USPQ 871 (CCPA 1981); In re Merk & Co., 800 F.2d 1091, 231 USPTQ 375 (Fed. Cir. 1986).

Conclusion

10. **THIS ACTION IS MADE FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication from the examiner should be directed to Clement Graham at (703) 305-1874. The examiner can normally be reached on Monday, Tuesday, and Wednesday from 5:30AM. to 6:OOPM.

10. If any attempt to reach the examiner by telephone is unsuccessful, the examiner's supervisor, Frantzy Poinvil can be reached on (703) 305-9779.

The Official Fax Number for TC-3600 is: (703) 305-7687

Clement Graham

Patent Examiner

December 5, 2002

FRANTZY POINVIL
PRIMARY EXAMINER
AU 3628